

FORM PTO-1599 (Modified)
(REV 11-2000)

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER

TRANSMITTAL LETTER TO THE UNITED STATES

T2146-907342

DESIGNATED/ELECTED OFFICE (DO/EO/US)

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR

CONCERNING A FILING UNDER 35 U.S.C. 371

09/869434

INTERNATIONAL APPLICATION NO.

INTERNATIONAL FILING DATE

PRIORITY DATE CLAIMED

PCT/FR00/02979

26 October 2000

28 October 1999

TITLE OF INVENTION

SAFE TERMINAL PROVIDED WITH A SMART CARD READER DESIGNED TO COMMUNICATE WITH A SERVER VIA AN INTERNET-TYPE NETWORK

APPLICANT(S) FOR DO/EO/US

Renaud MARIANA

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (24) indicated below.
4. ☒ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
 - a. ☒ is attached hereto (required only if not communicated by the International Bureau).
 - b. ☒ has been communicated by the International Bureau.
 - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
 - a. ☒ is attached hereto.
 - b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
 - a. ☐ are attached hereto (required only if not communicated by the International Bureau).
 - b. ☐ have been communicated by the International Bureau.
 - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
 - d. ☐ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
10. ☐ An English language translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).
11. ☐ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☒ A copy of the International Search Report (PCT/ISA/210).

Items 13 to 20 below concern document(s) or information included:

13. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
14. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☒ A **FIRST** preliminary amendment.
16. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
17. ☐ A substitute specification.
18. ☒ A change of power of attorney and/or address letter.
19. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
20. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
21. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
22. ☐ Certificate of Mailing by Express Mail
23. ☒ Other items or information:

Verification of Translation; PCT FORMS: Demand, PCT/RO/101; PCT/IB/301; PCT/IB/308
Proposed Drawing Corrections and 4 red-lined drawings

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR <div style="font-size: 1.5em; font-weight: bold; margin-top: 5px;">09/869434</div>	INTERNATIONAL APPLICATION NO. <div style="font-weight: bold; margin-top: 5px;">PCT/FR00/02979</div>	ATTORNEY'S DOCKET NUMBER <div style="font-weight: bold; margin-top: 5px;">T2146-907342</div>
--	--	---

24. The following fees are submitted:

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :		CALCULATIONS	PTO USE ONLY
<input type="checkbox"/> Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO	\$1000.00		
<input checked="" type="checkbox"/> International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO	\$860.00		
<input type="checkbox"/> International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO	\$710.00		
<input type="checkbox"/> International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4)	\$690.00		
<input type="checkbox"/> International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4)	\$100.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =		\$860.00	
Surcharge of \$130.00 for furnishing the oath or declaration later than _____ months from the earliest claimed priority date (37 CFR 1.492 (e)). <input type="checkbox"/> 20 <input type="checkbox"/> 30		\$0.00	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	10 - 20 =	0	x \$18.00		\$0.00
Independent claims	1 - 3 =	0	x \$80.00		\$0.00
Multiple Dependent Claims (check if applicable) <input type="checkbox"/>					\$0.00
TOTAL OF ABOVE CALCULATIONS =					\$860.00
<input type="checkbox"/> Applicant claims small entity status. (See 37 CFR 1.27). The fees indicated above are reduced by 1/2.					\$0.00
SUBTOTAL =					\$860.00
Processing fee of \$130.00 for furnishing the English translation later than _____ months from the earliest claimed priority date (37 CFR 1.492 (f)). <input type="checkbox"/> 20 <input type="checkbox"/> 30					\$0.00
TOTAL NATIONAL FEE =					\$860.00
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) (check if applicable). <input checked="" type="checkbox"/>					\$40.00
TOTAL FEES ENCLOSED =					\$900.00
					Amount to be refunded \$
					charged \$

a. ☒ A check in the amount of \$900.00 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 50-1165. A duplicate copy of this sheet is enclosed.

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Edward J. Kondracki
 MILES & STOCKBRIDGE P.C.
 Suite 500, 1751 Pinnacle Drive
 McLean, VA 22102-3833

SIGNATURE

Edward J. Kondracki
 NAME

20,604
 REGISTRATION NUMBER

June 28, 2001
 DATE

T2146-907342-US 3855/BC(PCT)

IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (D.O./E.O./US)

Applicant: Renaud MARIANA

International
Application No.: PCT/FR00/02979

International
Filing Date: 26 October 2000

U.S. Serial No.: To be Assigned

U.S. Filing Date: June 28, 2001

For: **SAFE TERMINAL PROVIDED WITH A SMART CARD
READER DESIGNED TO COMMUNICATE WITH A
SERVER VIA AN INTERNET-TYPE NETWORK**

McLean, Virginia

PRELIMINARY AMENDMENT

Honorable Commissioner of Patents
and Trademarks
Washington, D.C. 20231

Sir:

Please amend the subject application, filed concurrently herewith, as
indicated below:

IN THE TITLE:

Please cancel the title in its entirety and substitute the following new
title:

**-- SECURE TERMINAL PROVIDED WITH A SMART CARD READER
DESIGNED TO COMMUNICATE WITH A SERVER VIA AN INTERNET
NETWORK--**

IN THE SPECIFICATION:

After the title and before the first paragraph on page 1 at line 5, insert the following heading at the left-hand margin:

--FIELD OF THE INVENTION--;

Page 1, at line 8, insert the following heading at the left-hand margin:

--BACKGROUND OF THE INVENTION--;

Page 7, at line 31, before the paragraph beginning "While eliminating...", insert the following heading at the left-hand margin:

--SUMMARY OF THE INVENTION--;

Page 10, at line 16, before the paragraph beginning "The invention will now...", insert the following heading and sentence:

--BRIEF DESCRIPTION OF THE DRAWINGS--;

Page 11, before the first paragraph beginning "We will now...", insert the following paragraph at the left-hand margin:

--DESCRIPTION OF THE PREFERRED EMBODIMENT(S)--;

--While this invention has been described in conjunction with specific embodiments thereof, it is evident that many alternatives, modifications and variations will be apparent to those skilled in the art. Accordingly, the preferred embodiments of the invention as set forth herein, are intended to be illustrative, not limiting. Various changes may be made without departing from the true spirit and full scope of the invention as set forth herein and defined in the claims.—

IN THE CLAIMS:

Please amend claims 1 – 10. The claims that follow are a complete set of “clean” claims. The original claims marked up to show the changes with underlining and bracketing are included as an attachment to this Preliminary Amendment:

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214

1 1. A terminal equipped with a secure enclosure (6) designed to
2 communicate with at least one web server (4) via an internet network, using a
3 first Internet communication protocol, said secure enclosure comprising at
4 least one smart card reader, for reading a smart card storing at least one
5 software application, characterized in that said terminal (5) comprises a non-
6 secure part comprising at least a first communication node (50), said secure
7 enclosure (6) comprises at least a second communication node (60) and said
8 smart card (8) comprises at least a third communication node (80), said first,
9 second and third communication nodes (50, 60, 80) comprising, respectively,
10 first, second and third protocol stacks, each protocol stack comprising a given
11 number of software communication layers, and, respectively, first, second
12 and third pieces of specific software (64, 84), each comprising first software
13 entites (641, 841), said first software entities being paired two by two, wherein
14 said first node (50) authorizes at least communications between said terminal
15 (5) and said web server (4), using said first Internet communication protocol,
16 said first entities of said first and second pieces of specific software
17 authorizing the establishment of a bilateral data exchange session between
18 said terminal (5) and said secure enclosure (6), using a second given
19 communication protocol, in that said first entities (641, 841) of said second
20 (64) and third (84) pieces of specific software authorizing at least the
21 establishment of a bilateral data exchange session between said secure
22 enclosure (6) and said smart card (8), via said smart card reader, using a third
23 given communication protocol, so as to be able to connect at least one of said
24 software applications (A₁-A_n) of the smart card (8) with said web server (4).

1 2. A terminal according to claim 1, characterized in that said first
2 paired entities are constituted by intelligent agent software modules (641,
3 841), which establish said sessions.

1 3. A terminal according to claim 1, characterized in that said
2 terminal further comprises, in said non-secure part, at least one application
3 constituted by a web browser (51), and wherein said first Internet protocol is
4 the "HTTP/TCP-IP" protocol includes a URL address, comprising an IP
5 internet address element and a port number for the selection of said terminal
6 (5) and of an internal element of said terminal (5), and wherein said first entity
7 of said specific piece of software of said first communication node (50)
8 identifies said IP address element and said port number, and as a result of
9 said identification, data received from said web server (4) is routed to said
10 web browser (51), using said first Internet protocol, or translated and
11 transmitted to said second communication node (60) using said second given
12 communication protocol, in a first data transmission direction, and upon said
13 identification, data received from the second communication node (60) is
14 routed to said web browser (51) or to said web server (4) using said first
15 Internet protocol, in a second data transmission direction.

1 4. A terminal according to claim 3, characterized in that said
2 secure enclosure (6) also comprises at least one data entry keyboard (62)
3 and at least one enclosure HTTP server (61) disposed between said
4 keyboard (62) and said second communication node (60), said IP address

element and said port number being identified by said first entity (641) of said specific piece of software (64) of said second communication node (60) data received from said first communication node (50) being translated and again transmitted to said third communication node (80) using said third given communication protocol, in a first data transmission direction, and upon said identification, data received from the third communication node (80) is routed to said HTTP server (61), or translated and transmitted to said second communication node (50) using said second given protocol, in a second data transmission direction.

5. A terminal according to claim 4, characterized in that said secure enclosure comprises at least one additional computing resource (63) connected to said HTTP server (61) of the secure enclosure (6), and, said URL address comprising an additional address element, wherein upon identification of said additional address element, said HTTP server (61) selects said keyboard (62) or one of said additional computing resources (63).

6. A terminal according to claim 5, characterized in that said additional computing resource (63) is a biometric authentication device.

7. A terminal according to claim 4, characterized in that said smart card stores several software applications (A_1-A_n), card and HTTP server (81) disposed between said software applications (A_1-A_n) and said third node (80), and said card HTTP server (81) selectively activating at least one of said software applications (A_1-A_n) upon reception of a request coming from said

6 second node (60) or transmits the requests sent by said applications (A_1 - A_n)
 7 to said third communication node (80).

1 8. A terminal according to claim 7, characterized in that said smart
 2 card (8) also comprises a second software entity (ATS_1 - ATS_i) for interpreting
 3 an instruction set conveyed by said data received from said third
 4 communication node (80), and for translating said instruction set into a set of
 5 commands, said second software entity (ATS_1 - ATS_i) cooperating with said
 6 software applications (A_1 - A_n) and said specific piece of software (84) of said
 7 third communication node (80), said translated instruction set being
 8 associated with one of said software applications to be activated (A_1 - A_n) in
 9 said smart card (8).

1 9. A terminal according to claim 8, wherein said instruction set to
 2 be interpreted is constituted by a script, each of said second software entities
 3 being constituted by script translating intelligent agent (ATS_1 - ATS_i) software
 4 module.

1 10. A terminal according to claim 1, characterized in that a merchant
 2 software application (41) is stored in said web server (40), and said merchant
 3 software application (41) is adapted to be placed in interactive communication
 4 with at least one of said software applications (A_1 - A_n) of said smart card (8)
 5 via said first (50), second (60) and third communication nodes (80).

-- ABSTRACT

The invention concerns an architecture of a terminal (5) allowing communications between a smart card (8) and a web server (4), via an internet network (RI). The terminal (5) is equipped with a secure enclosure (6) comprising a smart card reader (8), a keyboard (62), and optionally, other computing resources (63). The non-secure part of the terminal (5) comprises a web browser (51) and a first communication node (50) that routes the requests received to the browser (51) or to the secure enclosure (6). The secure enclosure (6) comprises a second communication node (60) and an HTTP server (61). The smart card (8) comprises a third communication node (80) and an HTTP server (81). The web server (4) comprises a merchant application (41) that can be placed in communication with the smart card (8) and activate software applications (A₁-A_n) of the latter.--

REMARKS

This Preliminary Amendment is filed to insert headings to conform the application to U.S. practice and to correct informalities in the specification, claims and abstract resulting from a literal translation of the French text.


Early action on the merits is earnestly solicited.

Respectfully submitted,

MILES & STOCKBRIDGE P.C.

Date: June 28, 2001

By:


Edward J. Kondracki
Registration No. 20,604

1751 Pinnacle Drive – Suite 500
McLean, VA 22102-3833
Tel.: 703/903-9000
Fax: 703/610-8686

The following are the amended claims marked up to show the changes with underlining and bracketing:

1. (Amended) [Terminal] A terminal equipped with a secure enclosure (6) designed to communicate with at least one web server (4) via an internet network, using a first Internet communication protocol, said secure enclosure comprising at least one smart card reader, [said] for reading a smart card storing at least one software application, characterized in that said terminal (5) comprises a non-secure part comprising at least [a first module called] a first communication [mode] node (50), said secure enclosure (6) comprises at least [a second module called] a second communication node (60) and said smart card (8) comprises at least [a third module called] a third communication node (80), [in that] said first, second and third communication nodes (50, 60, 80) [comprise] comprising, respectively, first, second and third protocol stacks, each protocol stack comprising a given number of [so-called standard] software communication layers, and, respectively, first, second and third pieces of specific software (64, 84) , each comprising [at least one] first software [entity] entities (641, 841), said first software entities being paired two by two, [in that] wherein said first node (50) authorizes at least communications between said terminal (5) and said web server (4), using said first Internet communication protocol, [in that] said first entities of said first and second pieces of specific software [authorize] authorizing the establishment of a bilateral data exchange session between said terminal (5) and said secure enclosure (6), using a second given communication protocol,

22 in that said first entities (641, 841) of said second (64) and third (84) pieces of
 23 specific software [authorize] authorizing at least the establishment of a
 24 bilateral data exchange session between said secure enclosure (6) and said
 25 smart card (8), via said smart card reader, using a third given communication
 26 protocol, so as to be able to connect at least one of said software applications
 27 (A₁-A_n) of the smart card (8) with said web server (4).

1 2. (Amended) [Terminal] A terminal according to claim 1,
 2 characterized in that said first paired entities are constituted by intelligent
 3 agent software modules [called intelligent agents] (641, 841), which establish
 4 said sessions.

1 3. (Amended) [Terminal] A terminal according to claim 1,
 2 characterized in that [it] said terminal further comprises, in said non-secure
 3 part, at least one application constituted by a web browser (51), [in that] and
 4 wherein said first Internet protocol is the "HTTP/TCP-IP" protocol includes a
 5 [so-called] URL address, comprising [a so-called] an IP internet address
 6 element and a port number for the selection of said terminal (5) and of an
 7 internal element of [this] said terminal (5), [in that] and wherein said first entity
 8 of said specific piece of software of said first communication node (50)
 9 identifies said IP address element and said port number, [in that] and as a
 10 result of said identification, data received from said web server (4) is routed to
 11 said web browser (51), using said first Internet protocol, or translated and
 12 transmitted to said second communication node (60) using said second given
 13 communication protocol, in a first data transmission direction, and [in that]

14 upon said identification, data received from the second communication node
 15 (60) is routed to said web browser (51) or to said web server (4) using said
 16 first Internet protocol, in a second data transmission direction.

1 4. (Amended) [Terminal] A terminal according to claim 3,
 2 characterized in that said secure enclosure (6) also comprises at least one
 3 data entry keyboard (62) and at least one [so-called] enclosure HTTP server
 4 (61) disposed between said keyboard (62) and said second communication
 5 node (60), [in that said first entity (641) of said specific piece of software (64)
 6 of said second communication node (60) identifies] said IP address element
 7 and said port number[, in that] being identified by said first entity (641) of said
 8 specific piece of software (64) of said second communication node (60) data
 9 received from said first communication node (50) [is] being translated and
 10 again transmitted to said third communication node (80) using said third given
 11 communication protocol, in a first data transmission direction, and [in that]
 12 upon said identification, data received from the third communication node
 13 (80) is routed to said HTTP server (61), or translated and transmitted to said
 14 second communication node (50) using said second given protocol, in a
 15 second data transmission direction.

1 5. (Amended) [Terminal] A terminal according to claim 4,
 2 characterized in that said secure enclosure comprises at least one additional
 3 computing resource (63) connected to said HTTP server (61) of the secure
 4 enclosure (6), and [in that], said URL address comprising an additional
 5 address element, [said HTTP server (61),] wherein upon identification of said

- 6 additional address element, said HTTP server (61) selects said keyboard (62)
 7 or one of said additional computing resources (63).

- 1 6. (Amended) [Terminal] A terminal according to claim 5,
 2 characterized in that said additional computing resource (63) is a biometric
 3 authentication device.

- 1 7. (Amended) [Terminal] A terminal according to claim 4,
 2 characterized in that said smart card stores several software applications (A₁-
 3 A_n), [in that it comprises a so-called] card and HTTP server (81) disposed
 4 between said software applications (A₁-A_n) and said third node (80), and [in
 5 that] said card HTTP server (81) selectively [activates] activating at least one
 6 of said software applications (A₁-A_n) upon reception of a request coming from
 7 said second node (60) or transmits the requests sent by said applications (A₁-
 8 A_n) to said third communication node (80).

- 1 8. (Amended) [Terminal] A terminal according to claim 7,
 2 characterized in that said smart card (8) also comprises a second software
 3 entity (ATS₁-ATS_i) [capable of] for interpreting an instruction set conveyed by
 4 said data received from said third communication node (80), and [of] for
 5 translating [it] said instruction set into a set of commands, said second
 6 software entity (ATS₁-ATS_i) cooperating with said software applications (A₁-
 7 A_n) and said specific piece of software (84) of said third communication node
 8 (80), said translated instruction set being associated with one of said software
 9 applications to be activated (A₁-A_n) in said smart card (8).

1 9. (Amended) [Terminal] A terminal according to claim 8,
 2 [characterized in that,] wherein said instruction set to be interpreted [being] is
 3 constituted by a script, each of said second software entities [is] being
 4 constituted by [a software module called a] script translating intelligent agent
 5 (ATS₁-ATS) software module.

1 10. (Amended) [Terminal] A terminal according to claim 1,
 2 characterized in that a merchant software application (41) is stored in said
 3 web server (40), and said merchant software application (41) [stores a so-
 4 called merchant software application (41) designed] is adapted to be placed
 5 in interactive communication with at least one of said software applications
 6 (A₁-A_n) of said smart card (8) via said first (50), second (60) and third
 7 communication nodes (80)

Verification of Translation

I, Robin Holding, having an office at 948 15th Street, #4, Santa Monica, CA 90403-3134, hereby state that I am well acquainted with both the English and French languages and that to the best of my knowledge and ability, the appended document is a true and faithful translation of

Int'l. Patent Application No. PCT/FR00/02979

In the name of BULL CP& Inventor: Renaud MARIANA

Filed on October 26, 2000

I further declare that the above statement is true; and further, that this statement is made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent resulting therefrom.

June 22, 2001

Date

Robin Holding
Robin Holding

**SAFE TERMINAL PROVIDED WITH A SMART CARD READER
DESIGNED TO COMMUNICATE WITH A SERVER VIA AN INTERNET-
TYPE NETWORK**

5 The invention relates to an architecture of a terminal, more specifically a terminal of the type using a keyboard and a smart card reader located in a secure enclosure, and designed to communicate with a server via an internet network.

A device of this type is known, for example, by the trade name "safepad."

10 In the context of the invention, the term "terminal" should be understood in a general sense. The aforementioned terminal can specifically be constituted by a personal computer running on various operating systems, such as WINDOWS or UNIX (both of which are registered trademarks). It can also be constituted by a workstation, a portable computer or a so-called dedicated card terminal.

15 Likewise, in the context of the invention, the term "internet network" includes, in addition to the Internet *per se*, private enterprise networks or the like, known as "intranets," and the networks that extend them to the outside, known as "extranets."

20 Smart cards are used in various fields: banking and health care applications, as so-called electronic "purses," etc. Moreover, several applications can coexist in a smart card (a multi-application smart card).

25 For these types of applications, smart cards can be assigned various functions. In particular, they can be used for security purposes. The term "security" should be understood in a general sense, including confidentiality and/or the authentication of the user of the station and/or the holder of the smart card itself.

In the more specific context of these applications, the terminal can be equipped with a secure enclosure comprising a smart card reader, a keyboard and possibly one or more other computing resources.

Fig. 1 schematically illustrates the architecture of a terminal of the aforementioned type, according to the prior art.

30 To illustrate the concepts, it is assumed that the terminal 1 is basically constituted by a microcomputer. It is equipped with all the usual devices constituting such computing equipment and required for their proper operation (which are not represented): central processor, RAM, mass storage (hard disk), reader(s) information media (diskettes, etc.). In the particular case illustrated in Fig. 1, the terminal 1 is

equipped with a secure enclosure 3 comprising a smart card 2 reader 30 and a keyboard 31. The keyboard 31 is specifically used to enter data for authenticating the holder of the smart card 2: for example a password associated with an identifier of the smart card 2. Various electronic circuits allow communication between the secure
5 elements present inside this enclosure, including the keyboard 31 and the smart card 2 (via the reader 30), and between these secure elements and the non-secure elements present in the terminal 1.

Normally, the terminal comprises, in its non-secure part, a specific application
10 10, which will be hereinafter be called a "merchant" application, which handles the management and control of specific transactions permitted by the terminal 1 in question. Communications between this application 10 and the elements inside the secure enclosure 3 normally take place in accordance with a standard of the RS232 type. Communications between the elements inside the secure enclosure 3, including
15 a resident application 300, and the smart card 2, via the reader 3, normally take place in accordance with a protocol that complies with the ISO standards 7816-1 through 7816-4.

This type of architecture specifically has the following primary drawbacks:

- the merchant application installed in the terminal (non-secure part) and that residing in the secure enclosure are specific to this terminal;
- the associated computer programs are generally voluminous; and
- flexibility and reliability are limited, since any modification of these
20 programs requires a reloading of programs into the terminal (non-secure part) and into the secure enclosure, and thus possibly the execution of functional tests, which requires the presence of specialized personnel.

25 Generally, the latter operation must be repeated for a large number of terminals.

It must also be kept in mind that these applications must be fully or partially secure. It is therefore necessary to be able to guarantee, for the updating of the programs, a given level of security, appropriate for the specific application.

30 Most often, the terminal 1 is not isolated, in the sense that it is linked via a transmission network RI to one or more remote systems, one of which 4 is illustrated in Fig. 1. The nature of the network RI can vary, depending on the applications envisaged (banking, health care, etc.). It could be the Internet or a network of that

type (intranet or extranet), given the rapid growth of the latter type of network and the applications that use it. Normally, the overall architecture is of the so-called "client-server" type, the "server" generally being the remote system 4 and the "client" being the terminal 1. But under certain circumstances, the roles may be reversed or
5 alternated during the time of a transaction.

In an architecture of this type, the programs associated with the specific application 10 and the application 300, during a modification of their version for any reason whatsoever, can be updated in a centralized way, from one of the remote servers, for example the server 4. It follows that one of the drawbacks indicated can be alleviated, the update being performed by downloading. These operations,
10 however, require the implementation of administrative procedures that are well known. Moreover, the download can include sensitive data, or at least should not allow the installation into the terminal of programs and/or procedures that are unauthorized or dangerous for security (a "Trojan horse," "logical bombs," viruses, etc.).
15

Furthermore, with the increase in power and the universality of the Internet, there is a need to make the aforementioned specific applications, installed locally in the terminals, "migrate" to the remote servers, which will hereinafter be called "merchant servers," and to dialog directly with the smart card from these merchant
20 servers.

This second need, in particular, cannot be satisfied by the terminals of the prior art, for reasons that will be explained below.

But first, it seems useful to briefly describe a system architecture that allows communication between a terminal according to the prior art and a remote server, via
25 an internet network RI. An architecture of this type is represented schematically in Fig. 2, a figure in which the logical architecture of the terminal, references 1', is more particularly represented.

The terminal 1' in this case is a general type of terminal which may or may not be secure, this characteristic being unimportant for explaining the various types of
30 communication in question.

As indicated above, the terminal 1' naturally includes all the circuits and devices required for its proper operation, which are not represented in order to simplify the drawing. Normally, the terminal 1' is also connected to standard

peripherals, which may or may not be integrated, such as a display screen (not represented) and a keyboard 31, located in a secure enclosure (Fig. 1: 3) in the particular context of the invention.

Normally, communications in networks take place in accordance with protocols that comply with standards comprising several superposed software layers. In the case of an internet network RI, communications take place in accordance with protocols that are specific to this type of communication, but that also comprise several software layers. The communication protocol is chosen based on the application specifically envisaged: web page consultation, file transfers, e-mail, forms or news, etc.

The architecture of communication networks is described by various layers. For example, the OSI ("Open Systems Interconnection") standard defined by the ISO includes seven layers, which run from the so-called lower layers (for example the so-called "physical" layer that concerns the physical transmission medium) to the so-called upper layers (for example the so-called "application" layer), passing through intermediate layers, including the so-called "transport" layer. A given layer offers services to the layer that is immediately above it and requires other services from the layer that is immediately below it, via appropriate interfaces. The layers communicate by means of primitives. They can also communicate with layers on the same level. In certain architectures, one or another of these layers may be nonexistent.

In an Internet environment, there are five layers, and more precisely, going from the top layer to the bottom layer: the applications layer (http, ftp, email, etc.), the transport layer (TCP), the network address layer (IP), the data link layer (PPP, Slip, etc.) and the physical layer.

The terminal 1' includes circuits 11 for accessing the internet network. This could be a modem for connecting to a switched telephone line or an integrated services digital network (ISDN), for example via an Internet service provider (or ISP). The circuits 11 for accessing the network RI contain the lower software layers C₁ and C₂, which correspond to the aforementioned physical and data link layers.

Also represented are the upper layers C₃ and C₄, which correspond to the "network address" (IP) and "transport" (TCP) layers. The upper application layer (http, ftp, email, etc.) is represented schematically by a web browser NW of any type, preferably a standard type on the market.

The interface between the lower layers C_1 and C_2 and the upper layers C_3 and C_4 is constituted by a software layer 15, generally called a "lower level driver." The upper layers C_3 and C_4 are supported by this interface and are implemented by means of libraries of specific functions, or network libraries 14, with which they correspond.

5 In the case of the Internet, TCP/IP is implemented by means of libraries called "sockets."

This organization allows the browser NW to present requests to a remote server 4, in order to consult web pages (HTTP protocol), transfer files (FTP protocol), or send email (email protocol).

10 The terminal 1' also includes the card reader 30, located in a secure enclosure (Fig. 1: 3) in the particular context of the invention. To communicate with the smart card 2, the card reader 30 also includes two lower layers CC_1 (physical layer) and CC_2 (data link layer), which play a role similar to the layers C_1 and C_2 . The software interfaces with the layers CC_1 and CC_2 are described, for example, by the PC/SC specification ("Part 6, Service Provider"). The layers CC_1 and CC_2 themselves are
15 specifically described by the ISO standards 7816-1 through 7816-4.

An additional software layer 13 forms an interface between application layers, under the single reference $Appli_1$, and the lower layers CC_1 and CC_2 . The chief function devolved to this layer 13 is a multiplexing/demultiplexing function.

20 On the smart card 2 end, there is a similar organization, i.e., the presence of two lower layers, referenced CC'_1 (physical layer) and CC'_2 (data link layer), as well as an interface layer 23, entirely similar to the layer 13. This layer 23 provides an interface between the aforementioned protocol layers CC'_1 and CC'_2 and one or more application layers, represented in the form of a single module referenced $Appli_2$.

25 Communications between the smart card reader 30 and the smart card 2 take place by means of standard commands, known by the abbreviation APDU, for "Application Protocol Data Unit".

Various protocols can be used, including as non-exhaustive examples the following:

- 30
- the ETSI GSM 11.11 recommendation;
 - the protocol defined by the ISO 7816-3 standard, in character mode $T=0$;
 - the protocol defined by the ISO 7816-3 standard, in block mode $T=1$;

- or the protocol defined by the ISO 3309 standard, in HDLC (for High-Level Data Link Control procedure) frame mode.

Within the scope of the invention, the ISO 7816-3 protocol is preferably used, in block mode.

5 In an intrinsically known way, each protocol layer is associated with a certain number of primitives that allow data exchanges between layers of the same level and from one layer to another.

10 In the current state of the art, it is not possible to place the smart card in direct communication with a remote server 4 via the Internet RI, since the communication protocol with a standard type of smart card 2, as indicated above, is incompatible with those used in the Internet or in any network of this type. Nor is it possible to establish direct communications between the browser NW and the smart card 2, except by installing in the browser NW a piece of software, called a "plug-in," of a specific type.

15 Referring again to Fig. 1, assuming that the terminal 1 is linked to the Internet, and to summarize what has been mentioned above, it is noted that this terminal 1 according to the prior art, comprising a secure enclosure 3 equipped with a keyboard 31 and a smart card 2 reader 30, includes two main communication interfaces, S₁ and S₂, represented in dotted lines. A first interface S₁ links the enclosure 3 to the terminal 1 *per se* in which the merchant application 10 is run, and a second interface S₂ is provided for communications with the smart card 2. In reality, the interface S₂ is distributed between the application 300 and the smart card 2. Added to both of these 20 interfaces is the interface to the outside (Fig. 2: particularly the circuits 11), which allows the terminal 1 to communicate with the internet network RI. The interface S₁ accepts two levels of dialogue: a first, transparent dialogue for which a command sent 25 by the terminal 1 is executed without semantic modification by the interface S₂, and a second level of dialogue that involves the application 300.

30 Thus, the authentication by entering a password on the keyboard 31 is a command submitted to the interface S₁ that is interpreted by the application 300 and transformed into a series of exchanges via the interface S₂ between the application 300 and the smart card 2. The result of these exchanges is transmitted to the interface S₁.

Other than the fact that it is impossible, in the current state of the art, for a standard smart card 2 to accept direct exchanges with the Internet RI, as indicated

above, the major drawback of the terminals according to the prior art is constituted by the presence of the resident application 300. It is most often a so-called "proprietary" application, which means that the merchant application 10 must be written based on the characteristics and the type of the terminal used. It is therefore *a priori* different from one type of terminal to another, which does not facilitate maintenance operations. Moreover, it is not adapted to an Internet type of environment.

Standards have been proposed for applications of the same type as the invention, such as the standard known by the abbreviation OCF (for "Open Card Framework"), which attempts to standardize exchanges between the merchant terminal 1 and the smart card 2 reader 30 in compliance with, for example, the EMV standard for terminals. However, such a standard is not directly usable in an internet context.

There is also the so-called "C-SET" protocol, known in the field of banking applications defined by the GIE bank card. Using this protocol, a user connects to a merchant site available on the web and makes a purchase. During the transaction, the latter accesses elements of the secure enclosure in order to authenticate the holder of the bank card making the purchase. This authentication is performed by running software in the terminal (non-secure part) and the enclosure.

This protocol is not free of drawbacks, either:

- it requires the presence of specific software in the terminal and in the enclosure;
- it requires the certification of the software required by C-SET;
- the C-SET protocol is payment-oriented only; the software in the terminal that processes the information from the web server and from the bank card payment is payment software.

In these characteristics, it does not differ much from the solutions of the prior art mentioned above. It does not allow end-to-end communications using an Internet protocol, including direct addressing of the smart card. Given its specificity, it offers no flexibility and is not adapted for use in other fields: health care, updating of data stored in a smart card, point crediting, etc

While eliminating the drawbacks of the methods and architectures of the prior art, some of which have been mentioned, the object of the invention is to fulfill the needs that have arisen.

It promotes the utilization in the Internet of terminals comprising a secure enclosure equipped with at least a smart card reader and a keyboard, by allowing the migration of applications from smart card readers and terminals to a remote web server, and direct dialogue with the smart card.

5 It allows an updating or an addition of software in the secure enclosure, with maximum security.

To achieve this, according to a first aspect of the invention, the smart card is not addressed in standard fashion by APDUs in accordance with the aforementioned ISO 7816 communication protocol, but by using a URL address (for "Universal
10 Resource Locator"). As is known, a URL address is constituted by an IP address *per se* and a port number. In the same way, the secure enclosure uses this URL addressing.

According to one aspect of the invention, the smart card also acts like a web server and/or client.

15 The secure enclosure according to the invention is "transparent" for the internet network, in the sense that the "card commands" emanating from the remote merchant server do not involve elements for addressing the terminal. It follows that the resources associated with the secure enclosure are not accessible from the internet network. On the other hand, the applications contained in the smart card have the
20 capability to address and activate all the computing resources present in the secure enclosure, including a keyboard, by simply using URL addressing, as will be explained below.

To achieve this, the terminal physically comprises:

- a secure enclosure of a modified type, comprising at least a card reader and a
25 keyboard (and/or another computing resource), both of which are linked to a so-called secure-enclosure HTTP server, as well as an execution unit that manages all of the resources present in the enclosure; and

- in addition to the standard elements (memories, etc.) and a web browser, a first, so-called terminal communication node, which handles communications
30 between the internet network, the web browser and/or the secure enclosure.

Furthermore, the aforementioned secure enclosure comprises a second, so-called enclosure communication node, which handles communications between the

terminal itself, via the first communication node, the so-called secure-enclosure HTTP server, and/or the smart card reader.

The smart card itself is equipped with a third, so-called card communication node, and a software adaptation that acts like an HTTP server, forming an interface between at least one application resident in the smart card and the second communication node.

The first communication mode routes the requests from the internet network having a port number associated with the secure enclosure to this enclosure and performs the necessary protocol adaptations for placing the internet network in direct communication with the second communication node, and handles the propagation of information and/or orders to the smart card.

For certain applications, especially applications requiring a high level of security, the secure enclosure can advantageously comprise one or more additional computing resource(s), such as for example devices for biometric authentication (ocular recognition, voice and/or signature recognition), a coprocessor, or an external interpreter.

In a preferred variant of the method according to the invention, the programs required to run the elements and resources of the secure enclosure, or to update them, are downloaded via the internet network from a remote web server linked to this network. The update may include at least the partial erasure of these programs.

It is also possible, in additional variants of embodiment, to download, update and/or delete applications or parts of applications stored in the smart card (files, programs, scripts, etc.) via the internet network and the communication modes.

All of these operations can be performed under very good security conditions, due to the aforementioned transparency of the secure enclosure relative to the internet network.

Hence, the main object of the invention is a terminal equipped with a secure enclosure designed to communicate with at least one web server via an internet network, using a first Internet communication protocol, said secure enclosure comprising at least one smart card reader, said smart card storing at least one software application, characterized in that said terminal comprises a non-secure part comprising at least a first module called a first communication mode, said secure enclosure comprises at least a second module called a second communication node

and said smart card comprises at least a third module called a third communication node, in that said communication nodes comprise, respectively, first, second and third protocol stacks, each comprising a given number of so-called standard software communication layers, and respectively, first, second and third pieces of specific software, each comprising at least one first software entity, said first software entities being paired two by two, in that said first node authorizes at least communications between said terminal and said web server, using said first Internet communication protocol, in that said first entities of said first and second pieces of specific software authorize the establishment of a bilateral data exchange session between said terminal and said secure enclosure, using a second given communication protocol, in that said first entities of said second and third pieces of specific software authorize at least the establishment of a bilateral data exchange session between said secure enclosure and said smart card, via said smart card reader, using a third given communication protocol, so as to be able to connect at least one of said software applications of the smart card with said web server.

The invention will now be described in greater detail by referring to the attached drawings, in which:

- Fig. 1 schematically illustrates an example of a terminal according to the prior art comprising a secure enclosure equipped with a smart card reader and a keyboard;

- Fig. 2 illustrates, in a general way, the logical architecture of a terminal according to the prior art comprising a smart card reader and communicating with a web server via the internet network;

- Fig. 3 schematically illustrates an exemplary general architecture according to the invention allowing communications, via the internet network, between a remote so-called merchant server and a terminal equipped with a secure enclosure comprising a smart card reader, a keyboard and other computing resources;

- Fig. 4 illustrates the logical architecture of modules allowing communications between the secure enclosure of the terminal of Fig. 3 and the smart card; and

- Fig. 5 illustrates a particular embodiment of the logical architecture of the smart card.

We will now describe an exemplary embodiment of a terminal with a secure enclosure according to the invention and the system architecture for communication between this terminal and a so-called "merchant" server, with reference to Fig. 3.

The terminal, hereinafter referenced 5, can basically be embodied, as has been indicated, by a microcomputer or a similar device. It comprises a certain number of standard elements: microprocessor, RAM and ROM, mass storage (hard disk, etc.), etc., which are not represented and are well known to one skilled in the art. On the other hand, in the application specific to the invention, the terminal 5 comprises an enclosure 6, secured by physical and logical means that are intrinsically known. This secure enclosure 6 comprises elements common to the prior art, but also elements specific to the invention that will be indicated below. To begin with, it comprises, as in the prior art, a keyboard 62, its driver or "handler" 620, and a smart card reader 7.

The terminal 5 is connected to a remote server 4 via the Internet RI or any other network of this type (intranet, extranet). As in the case of Fig. 2, it comprises all of the software and hardware elements that make it possible to communicate using one of the protocols used on the Internet, including the HTTP/TCP-IP protocol. It is therefore unnecessary to describe these elements, except to mention that it includes a web browser, referenced 51. This browser 51 makes it possible, in particular, to present requests to the server 4. It constitutes one of the applications present in the terminal 5, which can actually include a plurality of applications.

According to a first characteristic of the invention, the applications specific to the merchant application have migrated to the server 4. The latter therefore specifically comprises an HTTP server *per se* 40 and the aforementioned merchant applications, stored in storage means 41.

According to another characteristic of the invention, the terminal comprises a first specific module 50, which will be called the first communication node, or "terminal communication node." This module 50 comprises standard communication means, including the protocol stacks described in connection with Fig. 2, but also specific elements that will be described below.

According to yet another characteristic, the secure enclosure 6 also comprises a specific module 50, which will be called the second communication node or "enclosure communication node."

The first communication node 50 makes it possible to make the servers of the network RI, for example the server 4, as well as the applications present in the non-secure part of the terminal 5 (for example the web browser 51) communicate with the elements present in the secure enclosure 6, including the smart card reader 7 and the smart card 8, via the second communication node 60.

The secure enclosure 6 comprises an HTTP server 61, which will be called the "enclosure HTTP server," disposed between the second communication node 60 and the keyboard 62. The latter constitutes one of the computing resources of the secure enclosure 6. The latter, as indicated in the preamble of the present specification, can comprise additional resources 1 through i, represented by the single reference number 63. These can include, for example, biometric authentication devices, a coprocessor or an external interpreter. The resource(s) 63 is (are) also connected to the HTTP server 61, in a way similar to the keyboard 62.

The server HTTP 61 is also connected to the smart card reader 7.

The communication node 60 makes it possible to route the requests from the terminal 5 to the smart card 8, via the smart card reader 7, and to route, in the opposite direction, the requests from the smart card 8, either to the HTTP server 61 or to the terminal 5, via the communication node 50.

According to one aspect of the invention, the HTTP server 61 allows the smart card 8, and it alone, to use the resources 62 through 63 of the secure enclosure 6.

The impossibility of accessing the information in the keyboard 62 or in the other resources 63, except than by passing through the smart card 8, which plays an intermediary role, is due to several factors:

a/ the enclosure 6 is physically secure (it is physically impossible to "spy" on the elements);

b/ the programming of the node 60 is such that it prevents any routing of data originating from outside the enclosure HTTP entity 61, the node 60 also being protected, since it is located inside the secure enclosure 6; and

c/ the programming of the enclosure HTTP entity 61 is such that the latter does not accept requests other than those emanating from the smart card 8, this server 61 also being protected, since it is also located inside the secure enclosure 6.

While point a/ itself is common to the prior art and to the invention, points b/ and c/ constitute specific and advantageous characteristics of the invention.

We will now describe in greater detail how communications take place between the internet network RI and the elements of the non-secure part of the terminal 5, between the latter and those of the secure terminal 6, between the elements of the secure terminal 6, and between the latter and the smart card 8 via the smart card reader 7.

According to one of the main characteristics of the invention, all of these communications take place in a mode that will be qualified as "homogeneous," entirely compatible with Internet protocols, using a standard URL address, and retaining the standardized communication protocols, particularly between the smart card 8 and the smart card reader 7 (i.e. in compliance with the aforementioned ISO 7816 standards).

The communications between the web browser 41 and the "merchant" server 4 do not pose any particular problems and can take place normally in accordance with the HTTP protocol, using standard protocol layers (see Fig. 2), and URL addressing. On the other hand, as has been mentioned, in the prior art, this is not true between the non-secure and secure elements of a terminal (Fig. 1: 1), in which communications normally take place in RS232 mode, or between the elements of the secure enclosure 6 and the smart card 8 via the reader 7. In the latter case, as explained in connection with Fig. 2, the communications do take place by implementing protocol layers, but with the help of a set of APDU orders, in compliance with the aforementioned ISO 7816-3 standard, hence in a way that is incompatible with an Internet protocol.

Also, the invention offers specific provisions that make it possible to unify the communications, while retaining the standardization of the elements involved in the communications and resulting in only minor modifications.

First of all, we will describe in detail the modifications to be made to the secure enclosure 6 and the smart card 8, so as to be able to handle communications between these two entities in a manner according to the invention.

According to one characteristic of the invention, the smart card 8 is equipped with a specific module constituting a third communication node 80 and an HTTP server 81, which will hereinafter be called the "card communication node" and the "card HTTP server," respectively. The n application(s) present in the smart card 8, A_1 through A_n , are connected through a first side of the HTTP server 81. With these

provisions, the smart card 8 is transformed into a web server and/or client for the secure enclosure 6 and can be "addressed" by a URL address.

This architecture is essentially obtained, according to the invention, by installing a first specific communication protocol layer into the smart card 8.

Likewise, a second specific communication protocol layer, forming the match of the first, is installed in the secure enclosure 6.

For the exchanges between the smart card 8 and the secure enclosure 6, the block diagram of Fig. 3 can be represented by the logical architecture illustrated by Fig. 4.

In this architecture, we find the protocol layers of the prior art, as illustrated by Fig. 2, which play the same roles and have the same references. It is therefore unnecessary to describe them again.

On the other hand, on either end, i.e., in the secure enclosure 6 and in the smart card 8, two additional specific protocol layers are provided, respectively 64 and 84.

In the secure enclosure 6, the specific layer 64 is interfaced with the protocol layers of the card reader 3, i.e., the lower layers CC₁ and CC₂, via the multiplexing layer 13. The specific layer 64 allows the transfer of data packets to and from the smart card 8. In addition, it adapts the existing applications for utilizations involving the smart card 8, without having to rewrite them.

On the smart card 8 end, there is an entirely similar organization, constituted by an additional instance of the specific layer, referenced 84, the match of the layer 64.

More precisely, the specific layers 64 and 84 are subdivided into three main software elements:

- a module, 640 or 840, for transferring blocks of information between the layers 13 and 23, via the conventional layers CC₁, CC₂, CC'₁ and CC'₂;
- one of more pieces of software called "intelligent agents," 641 or 841, which perform, for example, protocol conversion functions;
- and a module for managing the specific configuration, 642 and 842 respectively, a module that is comparable to a particular intelligent agent.

Therefore, in the secure enclosure 6 and the smart card 8, there is a communication protocol stack between the two entities.

The level-two entities (data link layers) CC₂ and CC'₂ handle the exchanges between the smart card 8 and the secure enclosure 6. These layers are responsible for detecting, and possibly correcting, transmission errors. The various protocols mentioned are usable for this purpose (the ETSI GSM 11.11 recommendation; the
5 protocol defined by the ISO 7816-3 standard, in character mode T=0 or in block mode T=1; or the protocol defined by the ISO 3309 standard, in HDLC frame mode). As indicated, within the context of the invention, the ISO 7816-3 protocol, in block mode, is preferably used.

In an intrinsically known way, each protocol layer is associated with a certain
10 number of primitives that allow data exchanges between layers of the same level and from one layer to another. For example, the primitives associated with the level-two layer are of the data request ("Data.request") type and data response by the card ("Data.response") type, as well as the data confirmation ("Data.confirm") type.

More particularly, the specific layers 64 and 84 are responsible for the
15 dialogue between the smart card 8 and the host, i.e., the secure enclosure 6. They also allow the establishment of a configuration adapted to the sending and/or reception of data packets.

As indicated above, the layers comprise three distinct entities.

The first entity, the module 640 or 840, is essentially constituted by a software
20 multiplexer. It allows the exchange of information between the smart card 8 and the host terminal 6, in the form of protocol data units. It plays a role similar to that of a data packet switcher. These units are sent or received via the level-2 layer (data link layer). This particular communication protocol makes it possible to place at least one pair of "intelligent agents" in communication. The first agent of each pair, 641, is
25 located in the layer 64 on the secure enclosure 6 end; the second, 841, is located in the layer 84, on the smart card 8 end. A link between two "intelligent agents" is associated with a session. A session is a two-way data exchange between these two agents.

An intelligent agent can perform all or some of the functions of the level three
30 and four layers, depending on the configuration implemented by the secure enclosure 6.

A particular intelligent agent is advantageously identified by a whole number, for example in 16 bits (a number between 0 and 65535). This identifier is used, for

example, in a protocol data unit constituting a destination reference and a source reference.

There are two main categories of intelligent agents: agents of the "server" type, which are identified by a fixed reference, and agents of the "client" type, which are identified by a variable reference, delivered by the configuration management module 642 or 842.

The process for opening a session is normally the following: an intelligent agent of the "client" type opens the session with an intelligent agent of the "server" type. The modules 642 and 842 manage tables (not represented) which contain a list of the intelligent agents present, on the host 6 end and smart card 8 end.

The intelligent agents, 641 or 841, are associated with particular properties or attributes. To illustrate the concept, and to give a non-limiting example, the following four properties are associated with intelligent agents:

- "host": agent located in the secure enclosure;
- "card": agent located in the smart card;
- "client": agent that initializes a session;
- "server": agent that receives a session request.

The intelligent agents make it possible to exchange data.

The configuration management modules, 642 and 842, respectively, are comparable, as has been indicated, to particular intelligent agents. For example, the module 642 on the host 6 side, specifically manages information related to the configuration of the secure enclosure 6 (operating modes), a list of the other agents present, etc. The module, 842, on the smart card 8 side, has similar functions. These two agents can be placed in communication with one another to establish a session.

According to one characteristic of the invention, the smart card 8 offers the host system, i.e. the enclosure 6, a virtual terminal model. To do this, the smart card 8 acts like a web server and/or client.

In a practical way, the smart card 8 is advantageously "addressed" using a URL address that defines a loopback to the terminal 5, and more particularly to the secure enclosure 6, and not a pointing to an external server like the server 4. For example, the structure of this URL is normally the following:

http://127.0.0.1:8080 (1) or
http://localhost:8080 (1a)

in which 127.0.0.1 is the IP loopback address ("localhost" being the literal translation of 127.0.0.1) and 8080 is the port number. The URL address of the resources 62 and/or 63 could be completed by a suffix of the "/xxx" type. For example, the management module 620 of the keyboard 62 could have the following as its URL address:

http://localhost:8080/kb (2)

The logical architecture that allows communications between the terminal 5 *per se* (between the nodes 50 and 60), i.e. the non-secure elements of the latter, and the secure enclosure 6 is similar to that represented in Fig. 4. Consequently, sessions can be established between the communication nodes 50 and 60 in accordance with the general schema that has just been described. The secure enclosure can particularly be addressed by a URL address, under the same port number as the smart card, or 8080 in the example described.

The communication node 50 also allows the terminal 5 to communicate with the internet network RI. Also, in addition to the properties associated with the intelligent agents, which are listed above, there are also the following two properties:

- "local": agent that does not communicate with the network;
- "network": agent that communicates with the network.

The terminal 5, in its entirety, is addressed by the same IP address as above. It hosts at least one so-called terminal application, advantageously the web browser 51. The latter is associated with a particular port.

For example, using a web page technique and hyperlinks, a user (not represented) can choose a product or a service from those available and transmit the request to the merchant server 4.

In addition to the web client-server function offered by the smart card 8, according to another aspect of the invention, included in the latter there is a mechanism similar to the so-called CGI (for "Common Gateway Interface") function installed in conventional web servers.

Before describing an exemplary architecture according to the invention that makes it possible to perform a function of this type, even in the smart card 8, it is useful to review the chief characteristics of a CGI operating mode.

CGI is a specification for implementing, from a web server, applications written for the UNIX (registered trademark), DOS or WINDOWS (registered

trademark) operating systems: By way of example, for the UNIX operating system, the specification is CGI 1.1 and for the Windows 95 operating system, the specification is CGI 1.3.

Again by way of example, an HTTP request for a URL address of the type

"http://www.host.com/cgi-bin/xxx" (3),

in which "host" refers to a host system (generally remote), is interpreted by a web server as the execution of a CGI-type command script named "xxx" and present in the directory "cgi-bin" of this host system. Although the directory can have any name *a priori*, by convention, this is the name given to the directory that stores scripts of the CGI type. A script is an instruction set of the operating system of the host system, whose final result is transmitted to the web browser that sent the aforementioned request or to any other application accessing the service, such as a merchant server. Various languages can be used to write this script, for example the language PERL (registered trademark).

In a practical way, the request is normally displayed on a computer screen in the form of a form contained in an HTML page. The language HTML makes it possible to post a form at a URL address. The form includes one or more fields, which may or may not be required, and which are filled in by a user using the usual entry means: a keyboard for text, a mouse for boxes to be checked or so-called "radio" buttons, etc. The contents of the form (and possibly so-called "hidden" information and instructions) is addressed to the web server. The HTML code of the page describes the physical structure of the form (frame, graphics, color and any other attribute), as well as the structure of the data fields to be filled in (name, length, data type, etc.).

The transmission can take place in two main types of HTTP formats. A first format uses the so-called "POST" method, and a second uses the so-called "GET" method. A piece of format type information is present in the code of the form page.

This mechanism, however, is not directly transposable to a smart card, even though the latter offers the web server functionality according to one of the characteristics of the invention.

We will now describe an exemplary architecture that makes it possible to activate any conventional type of application via a web server in the smart card, with reference to Fig. 5.

A merchant server 4 activates an HTTP request of the GET type at a URL address, which can be presented in the following way:

"http://@card:8080/xxx.8080/cgi-bin/le_cgi ? param1+param2" (4),

in which "@card" is the IP address of the terminal supporting the smart card (for example the loopback address "127.0.0.1" of the relation (1)), "le_cgi" is a particular CGI script to be executed in the smart card 8 and "param1" and "param2" are parameters to be entered into the aforementioned script. The request is first transmitted to the secure enclosure 6, via the communication nodes 50 and 60 (Fig. 3).

A session is established between the terminal and the smart card reader. Then another session is established between a pair of intelligent agents, 641 and 841, located in the specific layers of the secure enclosure 6 and the smart card 8, respectively 64 and 84. The data then passes through the packet multiplexer 640 of the specific communication protocol layer 64. It then passes through the standard protocol layers (see Fig. 2). However, in order to better illustrate certain specific aspects of the invention, which will be explained below, these layers are divided into two parts in Fig. 5: an APDU command handler 65a and lower protocol layers 65b (ISO 7816-3 standard).

Likewise, in the smart card 8, it passes through the lower protocol layers, referenced 85b, and the APDU command handler on the card end, referenced 85a, then the packet multiplexer 840, in order to be received by the intelligent agent 841, which will be called a "web agent."

It is appropriate to note that the data addressed to the web agent 841 are transported, in an intrinsically conventional way, in the form of APDU commands designed for the particular "packet multiplexer" application 840. The APDU command handler 85a selects this application in a way that is entirely similar to the other applications present in the smart card 8, A_1 through A_n . In other words, the packet multiplexer 840 is seen by the APDU command handler 85a as an ordinary card application.

The HTTP request is then analyzed by the web agent 841, which detects a reference to a particular directory, which will hereinafter be called "cgi-smart" by convention, and to a particular application, for example A_1 . The complete path in this case is therefore "cgi-smart/ A_1 ".

According to one characteristic of the method of the invention, the above entity designates a particular script associated with an equally particular application.

According to another aspect of the invention, particular intelligent agents are installed in the smart card 8, which will hereinafter be called "script translating agents," or in abbreviated fashion, "ATS." The script is then interpreted by one of the intelligent agents. This translation can be performed in various ways:

a/ by the web agent 841 itself, which in this case is equipped with a dual capacity;

b/ by a single script agent capable of translating all of the scripts present in the smart card 8;

c/ by a dedicated script agent which will hereinafter be called "ATSD" (one per script); or

d/ by an APDU agent 850a of the APDU command handler 85a, which in this case is equipped with a dual capacity.

The APDU agent 850a is a component of the APDU command handler layer 85a. The latter is a layer capable of centralizing all of the APDU commands sent and/or received by the system, of selecting applications from A_1 through A_n , but also of offering an intelligent agent type interface. It is therefore capable, according to one of the characteristics of the invention, of communicating with all of the intelligent agents (via sessions), whether these agents are located in the enclosure 6 or the smart card 8.

In case c/ above, a session is opened between the web agent 841 and one of the agents ATSD.

Fig. 5 illustrates an exemplary architecture for which the translating agents are of the "ATSD" type. They are referenced ATS_1 through ATS_n and associated with the applications A_1 through A_n . The selected application being assumed to be the application A_i , the session is established between the web agent 841 and the agent ATS_i .

A script translating agent generates a set of APDU commands. A session is opened between the translating agent, for example the agent ATS_i , and the APDU agent 850a. The orders are then sent to the APDU agent 850a. The APDU command handler 85a selects the "CGI" application A_i and transmits to it the APDU commands,

commands which are translated and therefore conventional, and which it is capable of understanding.

The responses from the application A_i are transmitted to the APDU command handler 85a, to the APDU agent 850a, then again to the agent ATS_i (and more generally to the script translating agent).

The various routings are represented symbolically in Fig. 5 by solid lines connecting the functional blocks, or by dotted lines inside these blocks.

To illustrate the concepts, without in any way limiting the scope of the present invention, the addressing technique having been defined in general terms up to this point, we will now describe in detail various possible routings, which will be called cases of utilization and which will be referenced CU-n:

CU-1: communication between the merchant server 4 and the smart card 8.

To achieve this, a URL address according to (1) is used. In this case, it is not necessary to use the keyboard 62. The request, transmitted via the internet network RI, arrives in the communication node 50. The latter identifies the port associated with the smart card, i.e. the port 8080, which is the same as that of the secure enclosure 6. The communication node 50 routes the request to the communication node 60. In all cases, no matter what the URL address, the latter routes the data packets received to the smart card 80. Finally, the latter activates one of the applications of the smart card 8, for example the application A_1 .

CU-2: communication between two applications of the smart card 8.

For example, the application A_1 wants to communicate with the application A_n . The request emanating from the application A_1 is routed through the HTTP server 81. In a practical way, a session is established between a pair of local intelligent agents in the smart card 8, in accordance with the schema described in connection with Fig. 4. The communication node 80 is not involved. There is no communication protocol adaptation to be performed.

CU-3: communication between a card application and the merchant application 41 in the server 4.

This case can occur especially when the smart card 8 has received a request from the merchant server 4 (case CU-1). A local application in the smart card 8, for example the application A_1 , can be activated. A given action, initiated by the received request, is then performed in the smart card, for example a CGI-type action, by

running a script or any equivalent process. This action is performed under the control of script-translating intelligent agents, as explained in connection with Fig. 5.

As a result, the application A_1 presents a request addressed to the server 4.

After examining the IP address, the HTTP server 81 routes the request to the communication node 80. A session is established between the smart card 8 and the secure enclosure 6, more precisely between the communication nodes 60 and 80, in accordance with the schema described in connection with Fig. 4. Likewise, the communication node 60, after examining the IP address, transmits the request to the communication node 50. The latter, after examining the IP address, in turn transmits the request via the internet network RI to its final destination, i.e. to the server 4.

The process can include several passes back and forth between the smart card 8 and the server 4, during the time of one transaction. When the process is finished (at the end of the CGI for example), the response from the smart card is transmitted to the merchant server 4, particularly via the successive communication nodes 80, 60 and 50.

CU-4: communication between a "card application" and a "terminal application."

For example, the application A_1 wants to communicate with a print manager (not represented) of the terminal and presents a request in this direction. After examining the IP address and the port number, the HTTP server 81 routes the request to the communication node 80. The request then follows the same path as in case CU-3, until it reaches the communication node 50. The latter, after examining the IP address and the port number, routes the request to the terminal application addressed, for example the print manager.

CU-5: communication between a "card application" and a resource of the secure enclosure.

It is assumed, first of all, in this case of utilization, that the smart card 8 is in "slave" mode relative to the merchant server 4 and that the latter has sent a request addressed to the smart card 8. This request is processed in the manner explained in cases CU-1 and CU-3. For example, a "merchant CGI" is executed in the smart card 8, in the manner described in connection with Fig. 5. This script is executed by activating one of the applications, for example A_i , with the help of one of the script translating agents, for example ATS_i . It is assumed that the merchant CGI needs

information entered on the keyboard 62 (a password for example) or other authentication information (from a biometric device constituting one of the resources 63). The CGI in question must be executed with a particular URL address. The application A_i sends a request whose address is, for example, the one given by (2) above. The presence of the suffix "/kb" tells the communication node 60 that it is necessary to loop the request back to the HTTP server 61, which in turn activates the driver 620 of the keyboard 62, and retrieves the awaited information (the entry of a password for example). The response to the request is transmitted, via the same path but in the opposite direction, to the smart card 8.

The response to the request from the merchant server 4 is then transmitted back to the latter. A back-and-forth dialogue can be established in a manner similar to case CU-3.

Several CGIs can be executed during the time of one transaction.

To illustrate the concepts, a first "merchant CGI" can result in the display, on a screen included in the secure enclosure 6 (one of the resources represented under the single reference 63), of a message prompting a user to compose a code and displaying an amount. A second CGI reads, for example, information transmitted by the keyboard 62. A third CGI can result, in this same display device, in a message of the "CODE CORRECT" type or any similar message.

CU-6: communication between the terminal and one of the resources of the secure enclosure.

For example, an application of the terminal 5 (in its non-secure part), for example the web browser 51, wants to communicate with one of the protected resources, for example with the keyboard 62, and sends a request in this direction.

The communication node 50 examines the URL address, identifies the port number of the secure enclosure 6 and transmits the request to it. The communication node 60, as a result of its programming, systematically routes the requests received, even if they are addressed to one of the resources inside the secure enclosure 6, to the smart card 8. At this stage, the request follows a path similar to case CU-1. It is the smart card 8 that determines whether there is a need to retransmit the request to the secure resource initially addressed, and possibly to modify it. The decision can result from an identification procedure involving the examination of security data stored in the smart card, particularly in a read-only memory, possibly in encrypted form. As in case CU-

4, an element outside the secure enclosure 6 never has direct access to the protected resources.

This last characteristic allows updates of software resident in the secure enclosure 6, additions or at least partial deletions of this software, in a way that is more reliable than in the prior art. In fact, it is customary to authenticate modifications of this nature from a key embedded in the software of the secure enclosure 6.

Since only the smart card 8 can access the protected resources of the secure enclosure 6 from the outside, the downloading of software resources can therefore be done from an Internet server, by means of the smart card, while retaining a high degree of security. The downloaded data, if they are sensitive, need only be suitably encrypted, using a robust algorithm and/or a long enough encryption key. As a result of the intermediary function played by the smart card 8, the mechanism implemented in the invention is *a priori* stronger than a simple embedding of a key in a storage device (not represented) of the secure enclosure 6.

It is also possible to modify the contents of the software resources of the secure enclosure 6 directly from a smart card 8, by downloading pieces of software stored in the latter. The volume of software thus downloaded is nevertheless limited by the resources specific to the smart card (storage capacity), which is not *a priori* the case with a download via an internet network from a web server, which server can be equipped with substantial computing resources. The download time is naturally dependent on the quantity of software to be downloaded, but the use of fast modems and/or high-speed communication lines tends to keep this time within limits that are entirely reasonable for the applications envisaged.

With the reading of the above, it is easy to see that the invention clearly achieves the objects set forth.

While maintaining the possibility of using conventional components and standardized communication modes, particularly between the secure enclosure and the smart card, via the reader, it specifically allows addressing and communications that are compatible with the HTTP internet protocol. It transforms the smart card into a web client-server, capable of performing operations of the CGI type. It specifically allows a direct and interactive addressing of the smart card from a web server via the internet network, or in the opposite direction. It does not require any specific merchant application in the terminal itself and in the secure enclosure. It offers a great

deal of flexibility and is easily adapted to various fields of application. It involves only minor modifications of the components used, which modifications can essentially be summarized as the installation of specific pieces of software, it being understood that the word "specific" does not indicate any dependency on the applications handled. In particular, the applications resident in the smart card are standard applications and do not require any rewriting. Moreover, the specific applications, from a "merchant application" point of view, are located entirely in the remote web server. The latter can contain a plurality of them. Because of this, it is easy to update and delete these applications, as well to add new applications. This characteristic offers great flexibility. The version of the programs is identical for all of the terminals that connect to the server. Finally, the security provided by the invention is very high. It is possible to use robust encryption algorithms and very long keys for communications through the internet network. Furthermore, according to one characteristic of the invention, all the requests originating from outside the secure enclosure, whether from the non-secure part of the terminal or directly from the Internet, must necessarily pass through the smart card and remain under its exclusive control. The latter alone decides, for example based on resident security data, what use should be made of these requests. And the smart card remains the property of the holder.

It should be clear, however, that the invention is not limited to just the exemplary embodiments explicitly described, particularly in relation to Figs. 3 through 5.

In one embodiment (not represented), the secure enclosure could contain only a smart card reader, the application(s) stored in the smart card being self-sufficient in authenticating the holder and/or allowing a transaction between the remote web server and the smart card. The keyboard could be omitted and replaced by one of the protected resources, such as a biometric device. Finally, it is possible to add, to the first smart card reader, a second smart card reader, or several.

CLAIMS

1 1. Terminal equipped with a secure enclosure designed to communicate
2 with at least one web server via an internet network, using a first Internet
3 communication protocol, said secure enclosure comprising at least one smart card
4 reader, said smart card storing at least one software application, characterized in that
5 said terminal (5) comprises a non-secure part comprising at least a first module called
6 a first communication mode (50), said secure enclosure (6) comprises at least a
7 second module called a second communication node (60) and said smart card (8)
8 comprises at least a third module called a third communication node (80), in that said
9 communication nodes (50, 60, 80) comprise, respectively, first, second and third
10 protocol stacks, each comprising a given number of so-called standard software
11 communication layers, and respectively, first, second and third pieces of specific
12 software (64, 84) , each comprising at least one first software entity (641, 841), said
13 first software entities being paired two by two, in that said first node (50) authorizes at
14 least communications between said terminal (5) and said web server (4), using said
15 first Internet communication protocol, in that said first entities of said first and second
16 pieces of specific software authorize the establishment of a bilateral data exchange
17 session between said terminal (5) and said secure enclosure (6), using a second given
18 communication protocol, in that said first entities (641, 841) of said second (64) and
19 third (84) pieces of specific software authorize at least the establishment of a bilateral
20 data exchange session between said secure enclosure (6) and said smart card (8), via
21 said smart card reader, using a third given communication protocol, so as to be able to
22 connect at least one of said software applications (A₁-A_n) of the smart card (8) with
23 said web server (4).

1 2. Terminal according to claim 1, characterized in that said first paired
2 entities are constituted by software modules called intelligent agents (641, 841),
3 which establish said sessions.

1 3. Terminal according to claim 1, characterized in that it comprises, in
2 said non-secure part, at least one application constituted by a web browser (51), in
3 that said first Internet protocol is the "HTTP/TCP-IP" protocol includes a so-called

URL address, comprising a so-called IP internet address element and a port number for the selection of said terminal (5) and of an internal element of this terminal (5), in that said first entity of said specific piece of software of said first communication node (50) identifies said IP address element and said port number, in that as a result of said identification, data received from said web server (4) is routed to said web browser (51), using said first Internet protocol, or translated and transmitted to said second communication node (60) using said second given communication protocol, in a first data transmission direction, and in that upon said identification, data received from the second communication node (60) is routed to said web browser (51) or to said web server (4) using said first Internet protocol, in a second data transmission direction.

4. Terminal according to claim 3, characterized in that said secure enclosure (6) also comprises at least one data entry keyboard (62) and at least one so-called enclosure HTTP server (61) disposed between said keyboard (62) and said second communication node (60), in that said first entity (641) of said specific piece of software (64) of said second communication node (60) identifies said IP address element and said port number, in that data received from said first communication node (50) is translated and again transmitted to said third communication node (80) using said third given communication protocol, in a first data transmission direction, and in that upon said identification, data received from the third communication node (80) is routed to said HTTP server (61), or translated and transmitted to said second communication node (50) using said second given protocol, in a second data transmission direction.

5. Terminal according to claim 4, characterized in that said secure enclosure comprises at least one additional computing resource (63) connected to said HTTP server (61) of the secure enclosure (6), and in that, said URL address comprising an additional element, said HTTP server (61), upon identification of said additional address element, selects said keyboard (62) or one of said additional computing resources (63).

6. Terminal according to claim 5, characterized in that said additional computing resource (63) is a biometric authentication device.

7. Terminal according to claim 4, characterized in that said smart card stores several software applications (A_1-A_n), in that it comprises a so-called card HTTP server (81) disposed between said software applications (A_1-A_n) and said third node (80), and in that said card HTTP server (81) selectively activates at least one of said software applications (A_1-A_n) upon reception of a request coming from said second node (60) or transmits the requests sent by said applications (A_1-A_n) to said third communication node (80).

8. Terminal according to claim 7, characterized in that said smart card (8) also comprises a second software entity (ATS_1-ATS_i) capable of interpreting an instruction set conveyed by said data received from said third communication node (80), and of translating it into a set of commands, said second software entity (ATS_1-ATS_i) cooperating with said software applications (A_1-A_n) and said specific piece of software (84) of said third communication node (80), said translated instruction set being associated with one of said software applications to be activated (A_1-A_n) in said smart card (8).

9. Terminal according to claim 8, characterized in that, said instruction set to be interpreted being constituted by a script, each of said second software entities is constituted by a software module called a script translating intelligent agent (ATS_1-ATS_i).

10. Terminal according to claim 1, characterized in that said web server (40) stores a so-called merchant software application (41) designed to be placed in interactive communication with at least one of said software applications (A_1-A_n) of said smart card (8) via said first (50), second (60) and third communication nodes (80).

**SAFE TERMINAL PROVIDED WITH A SMART CARD READER
DESIGNED TO COMMUNICATE WITH A SERVER VIA AN INTERNET-
TYPE NETWORK**

Inventor: Renaud MARIANA

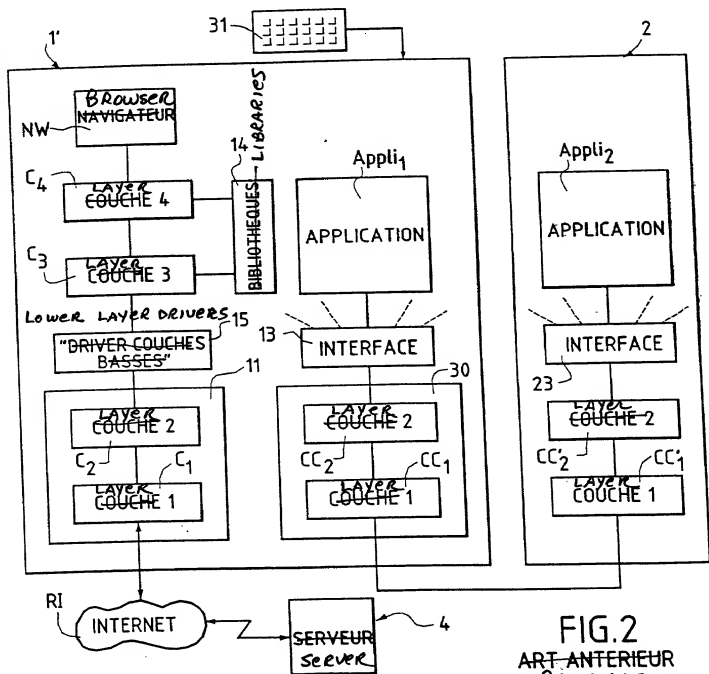
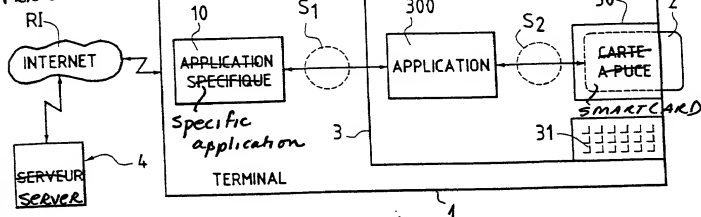
Applicant: BULL CP8

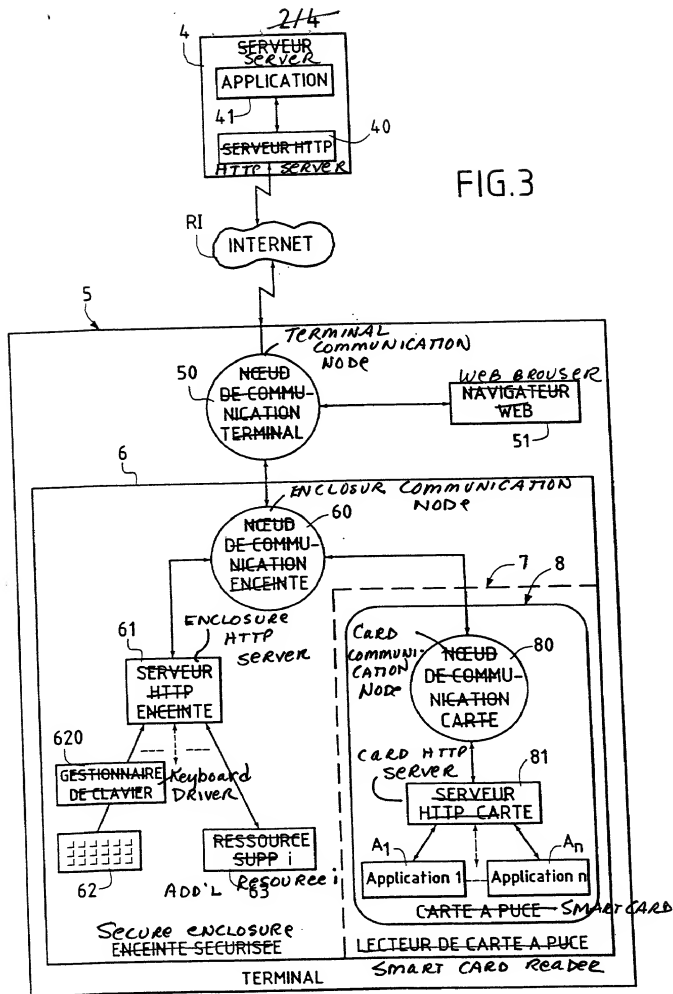
ABSTRACT

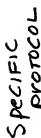
The invention concerns an architecture of a terminal (5) allowing communications between a smart card (8) and a web server (4), via an internet network (RI). The terminal (5) is equipped with a secure enclosure (6) comprising a smart card reader (8), a keyboard (62), and optionally, other computing resources (63). The non-secure part of the terminal (5) comprises a web browser (51) and a first communication node (50) that routes the requests received to the browser (51) or to the secure enclosure (6). The secure enclosure (6) comprises a second communication node (60) and an HTTP server (61). The smart card (8) comprises a third communication node (80) and an HTTP server (81). The web server (4) comprises a merchant application (41) that can be placed in communication with the smart card (8) and activate software applications (A₁-A_n) of the latter.

FIG. 3

FIG.1

ART ANTERIEUR
PRIOR ART





protocol
layer
couche de
protocole
spécifique

64 } management module / DE GESTION

INTELLIGENT
AGENT
AGENT
INTELLIGENT

INTELLIGENCE

MULTIPLIXEUR
LOGICIEL
SOFTWARE
MULTIPLIXER 1:

MULTI PLEXER

INTERFACE

1 FT FTR Reader

7-

COUCHÉ 2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----

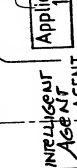
27-

1-713(06)

Secure enclosure
INFANT FURFURISEE

TERMINAL

56



Application 1

Application n

~~COUCHE DE~~ S
~~PROTOCOLE~~ P
~~SPECIFIQUE~~ L

management module

MULTIPLIXEUR LOGICIEL
SOFTWARE MULTIPLEXER

23 INTERFACE

Q

—

LAYER
CONTENTS

7

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----

LAYER	
-------	--

1. 247007

~~CARTE~~ Smart
~~APUÉE~~ CARD

FIG. 4

4/4

SCRIPT TRANSLATING AGENTS

AGENTS TRANSDUCTEURS DE SCRIPT

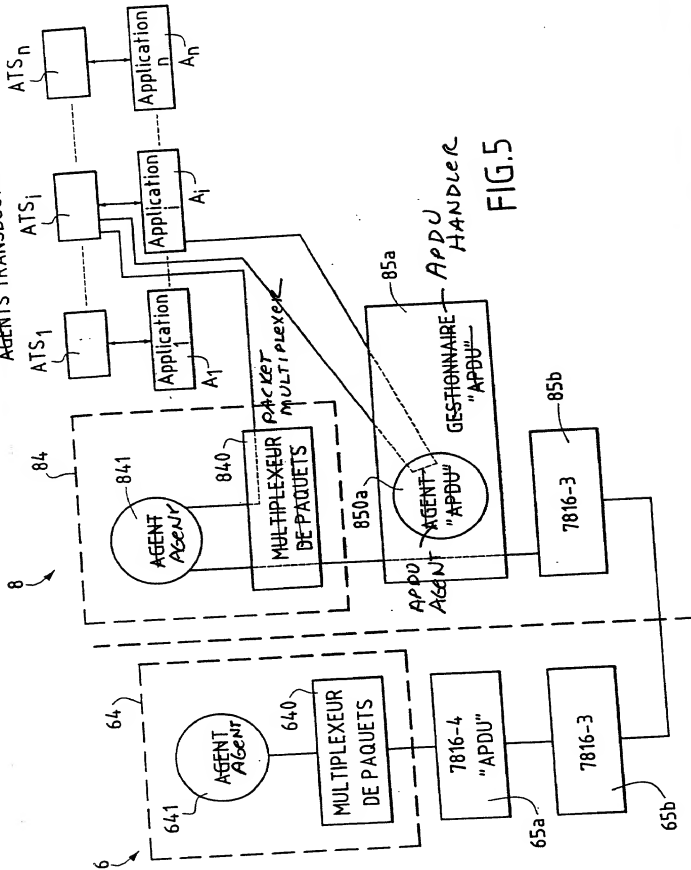


FIG.5

Declaration and Power of Attorney For Patent Application

Declaration Pour Demandes de Brevets Avec Pouvoirs

French Language Declaration

En tant qu'inventeur nommé ci-après, Je déclare par le présent acte que:

Mon nom, mon domicile, mon adresse postale, ma nationalité sont ceux qui figurent ci-après,

Je déclare que je crois être l'inventeur original, premier et unique (si un seul nom figure sur le présent acte) ou un des co-inventeurs, originaux et premiers (si plusieurs noms figurent sur le présent acte) du sujet revendiqué et pour lequel un brevet est demandé sur la base de l'invention intitulée:

Terminal sécurisé muni d'un lecteur de carte à puce destiné à communiquer avec un serveur via un réseau de type Internet

dont la description
(cocher la case correspondante)

☒ est annexée au présent acte.

☐ a été déposée _____

Numéro de série de la demande _____

et modifiée le _____
(si approprié)

Je déclare par le présent acte avoir examiné et compris le contenu de la description identifiée ci-dessus, revendications y compris, et le cas échéant telle que modifiée par l'amendement cité plus haut.

Je reconnais le devoir de divulguer l'information qui est en rapport avec l'examen de cette demande selon Titre 37 du Code des Règlements Fédéraux §1.56(a).

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

the specification of which

(check one)

☐ is attached hereto.

☐ was filed on _____ as

Application Serial No. _____

and was amended on _____
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

French Language Declaration

Je revendique par le présent acte le bénéfice de priorité étrangère selon Titre 35, du Code des Etats-Unis, §119 de toute demande de brevet ou d'attestation d'inventeur énumérée ci-après, et j'ai identifié également ci-après toute demande étrangère de brevet ou d'attestation d'inventeur ayant une date de dépôt antérieure à celle de la demande pour laquelle la priorité est revendiquée.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior foreign applications

Demande(s) de brevet antérieure(s) dans un autre pays:

FR 99 13508

France

28 10 1999

(Number)
(Numéro)

(Country)
(Pays)

(Day/Month/Year Filed)
(Jour/Mois/Année de dépôt)

(Number)
(Numéro)

(Country)
(Pays)

(Day/Month/Year Filed)
(Jour/Mois/Année de dépôt)

(Number)
(Numéro)

(Country)
(Pays)

(Day/Month/Year Filed)
(Jour/Mois/Année de dépôt)

Priority claimed

Droit de priorité
revendiqué

☒ Yes
Oui

☐ No
Non

☐ Yes
Oui

☐ No
Non

☐ Yes
Oui

☐ No
Non

Je revendique par le présent acte, le bénéfice selon Titre 35 du Code des Etats-Unis, §120 de toute(s) demande(s) américaine(s) énumérée(s) ci-après et, dans la mesure où le sujet de chacune des revendications de cette demande n'est pas divulgué dans la demande américaine antérieure, de la façon définie par le premier paragraphe de Titre 35 du Code des Etats-Unis, §112, je reconnais le devoir de divulguer l'information pertinente selon Titre 37 du Code des Règlements Fédéraux, §1.56(a), toute information qui se présente entre la date de dépôt de la demande antérieure et la date de dépôt de la demande, soit nationale, soit internationale PCT.

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

PCT/FR 00/02879

(Application Serial No.)
(No. de Demande)

28/10/00

(Filing Date)
(Date de Dépôt)

PENDING

(Etat)
(brevetée, pendante,
abandonnée)

(Status)
(patented, pending,
abandoned)

(Application Serial No.)
(No. de Demande)

(Filing Date)
(Date de Dépôt)

(Etat)
(brevetée, pendante,
abandonnée)

(Status)
(patented, pending,
abandoned)

Je déclare par le présent acte que toutes mes déclarations, à ma connaissance, sont vraies et que toutes les déclarations faites à partir de renseignements ou de suppositions, sont tenues pour être vraies; de plus, toutes ces déclarations ont été faites en sachant que de fausses déclarations volontaires ou autres actes de même nature sont sanctionnées par une amende ou un emprisonnement, ou les deux, selon la Section 1001, du Titre 18 de Code des Etats-Unis et que de telles déclarations délibérément fausses peuvent compromettre la validité de la demande ou du brevet délivré.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

French Language Declaration

POUVOIR: En tant qu'inventeur, je désigne l'(les) avocat(s) et/ou l'(les) agent(s) suivant(s) pour poursuivre la procédure de cette demande et traiter toute affaire la concernant supris du Bureau des Brevets et de Marques:

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)

10 Harold L. Stowell, Reg. 17,233
Edward J. Kondracki, Reg. 20,604
Dennis P. Clarke, Reg. 22,549
William L. Feeney, Reg. 29,918
John C. Kerins, Reg. 32,421

Harold L. Stowell, Reg. 17,233
Edward J. Kondracki, Reg. 20,604
Dennis P. Clarke, Reg. 22,549
William L. Feeney, Reg. 29,918
John C. Kerins, Reg. 32,421

Adresser toute correspondance à:

☐ Edward J. Kondracki, Esq.
☐ KERMAM, STOWELL, KONDRACKI
☐ & CLARKE, P.C.
☐ 5203 Leesburg Pike, Suite 600 -
☐ Falls Church, VA 22041

Send Correspondence to:

Edward J. Kondracki, Esq.
KERMAM, STOWELL, KONDRACKI
& CLARKE, P.C.
5203 Leesburg Pike, Suite 600
Falls Church, VA 22041

Adresser toute communication téléphonique à:
(Nom) (Numéro de téléphone)

☐ Edward J. Kondracki, Esq.
☐ (703) 998-3302

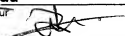
Direct Telephone Calls to: (name and telephone number)

Edward J. Kondracki, Esq.
(703) 998-3302

Nom complet du seul ou premier inventeur

MARIANA Renaud

Full name of sole or first inventor

Signature de l'inventeur  Date 5/11/99

Inventor's signature Date

Domicile
5 Square Las Cases 78150 LE CHESNAY FRANCE FR

Residence

Nationalité
Française

Citizenship

Adresse Postale
5 Square Las Cases 78150 LE CHESNAY FRANCE

Post Office Address

Nom complet du second co-inventeur, le cas échéant

Full name of second joint inventor, if any

Signature de l'inventeur Date

Second inventor's signature Date

Domicile

Residence

Nationalité

Citizenship

Adresse Postale

Post Office Address

(Fournir les mêmes renseignements et la signature de tout co-inventeur supplémentaire.)

(Supply similar information and signature for third and subsequent joint inventors.)

T2146-907342-US 3855/BC(PCT)

IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (D.O./E.O./US)

Applicant: Renaud MARIANA

International
Application No.: PCT/FR00/02979

International
Filing Date: 26 October 2000

U.S. Serial No.: To be Assigned

U.S. Filing Date: June 28, 2001

For: **SECURE TERMINAL PROVIDED WITH A SMART
CARD READER DESIGNED TO COMMUNICATE
WITH A SERVER VIA AN INTERNET NETWORK**

McLean, Virginia

CHANGE OF ADDRESS

Honorable Commissioner of Patents and Trademarks
Washington, D.C. 20231

Sir:

Effective immediately, please note our new correspondence address
and telephone/fax numbers as follows:

Miles & Stockbridge P.C.
1751 Pinnacle Drive
Suite 500
McLean, VA 22102-3833
Telephone: 703-903-9000
Fax: 703-610-8686

Respectfully submitted,

MILES & STOCKBRIDGE P.C.

Date: June 28, 2001

By: 

Edward J. Kondracki
Registration No. 20,604

1751 Pinnacle Drive – Suite 500
McLean, VA 22102-3833
Tel.: 703/903-9000